PATENT APPLICATION

LIT3-BI13

INTEGRATED OPTICS ENCRYPTION DEVICE

Michael L. Bean
Lawrence E. Bean
George A. Pavlath
Eric Lee Goldner

INTEGRATED OPTICS ENCRYPTION DEVICE

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The present invention relates generally to an encryption device. More particularly, the present invention relates to the encryption of a signal through use of a multi-functional integrated optics chip or MIOC.

BACKGROUND ART

The ability to encrypt and decrypt data is becoming increasingly important as e-mail, data files, voice transmissions, and other transmissions travel the Internet. The majority of encryption algorithms focus on encryption of data using software techniques and complex protocols such as a public key/private key system. The software reads plain text and translates it into crypto-text according to the encryption algorithm. The crypto-text is then generally transmitted to another location where a software program uses a key applied to the crypto-text to decrypt the data.

These software methods can be slow and cumbersome particularly regarding the demands that can be made on computer processors by encryption and decryption software. This type of encryption is also vulnerable to unauthorized decryption. For example, the public key/private key system is an asymmetric encryption algorithm. The encryption key is generally available to the public and is therefore vulnerable to chosen-plaintext attacks. Also, the public key/private key system requires the use of prime numbers, increasingly large prime numbers for improved security. Prime numbers become scarcer as they increase in size and require an increasing amount of computational time to obtain. Thus, a high-speed

hardware-based encryption device that does not rely on the use of prime numbers is desirable.

SUMMARY OF THE INVENTION

Sub a1

~~The present invention relates generally to an integrated optics encryption~~ device. The preferred embodiment of the invention is an integrated optics encryption device comprising a coherent light source connected to a multi-functional integrated optics chip (MIOC). The MIOC comprises two divergent paths with mirrored ends. The MIOC also has an encrypted message output. One path is connected to a message signal input that can alter the refractive index of the path. The other path is connected to a key signal input that can alter the refractive ~~index of the other path.~~

The preferred embodiment of the invention also lends itself to a useful method for encryption using interference from a coherent light source comprising the steps of:

issuing a coherent light signal from a coherent light source through a fiber optic connection to a multi-functional integrated optics chip;

dividing the light signal into two paths within the multi-functional integrated optics chip;

issuing pre-determined signals to the paths of the multi-functional integrated optic chip where a message signal input is attached to one path of the multi-functional integrated optics chip and a key signal input is attached to the other path;

recombining the divided light signal to create an encrypted signal; and,

outputting the encrypted signal via an encrypted message output.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects and features of the present invention, which are believed to be novel, are set forth with particularity in the appended claims. The present invention, both as to its organization and manner of operation, together with further objects and advantages, may best be understood by reference to the following description, taken in connection with the accompanying drawings.

Figure 1 is a circuit diagram of a preferred embodiment of the invention.

Figure 2 is a signal diagram of various signal inputs and outputs of the invention.

Figure 3 is a table for a basic encryption key used with a preferred embodiment of the invention.

Figure 4 is a diagram of an alternative preferred embodiment of the invention.

Figure 5 is a diagram of an alternative preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Sub a2

~~The following description is provided to enable any person skilled in the art~~ to make and use the invention and sets forth the best modes contemplated by the inventor of carrying out his invention. Various modifications, however, will remain readily apparent to those skilled in the art, since the general principles of the present invention have been defined herein specifically to provide an integrated optics encryption device.

Referring now to Figure 1, a preferred embodiment of an integrated optics encryption device 10 comprises a coherent light source 20. In the preferred embodiment, the coherent light source 20 is a laser, including but not limited to a laser diode. The coherent light source 20 is connected by fiber optic link 25 to a

multi-functional integrated optics chip (MIOC) 30. The MIOC 30 in the preferred embodiment comprises a lithium-niobate chip. In the embodiment of Figure 1, the MIOC 30 comprises two divergent paths 40 and 50 with ends 45 and a loop 60. The MIOC also has an encrypted message output 70.

Referring to Figure 4, the MIOC 30 in an alternative embodiment comprises two divergent paths 40 and 50 with ends 45, each end 45 being mirrored to reflect light signals. In a preferred embodiment, each end 45 is coated with a metallic film or a multi-layer dielectric film to form a reflector for each path 40 and 50. Referring to Figure 5, the MIOC 30 in another alternative embodiment comprises two divergent paths 40 and 50 meeting at a convergent end 47 connected to the encrypted message output 70.

In each embodiment, one path 40 is controlled by a message signal input 80 that can reversibly alter the refractive index of the path 40. The message signal input 80 is preferably a metal pad attached to the MIOC 30 that receives signals that change the voltage of the pad and alters the refractive index of the MIOC 30, including the path 40. By altering the refractive index of the path 40, the message signal input can either allow a light signal to pass through the path 40 or destructively interfere with, or cancel, the signal. The message signal input 80 is typically connected to message signal generating means such as a pulse signal generator, computer or any other source of digital signal input.

In each embodiment, one path 50 is controlled by a key signal input 90 that can reversibly alter the refractive index of the path 50. The key signal input 90 is preferably a metal pad attached to the MIOC 30 that receives signals that change the voltage of the pad and alters the refractive index of the MIOC 30, including the path 50. By altering the refractive index of the path 50, the key signal input can

either allow a light signal to pass through the path 50 or destructively interfere with, or cancel, the signal. The key signal input 90 is typically connected to a key signal generating means such as a pulse signal generator, computer or any other source of digital signal input. It can also be connected to another MIOC. It is preferred that the key signal generating means act as a random number generator.

One embodiment of the encryption process is shown in Figure 2. A message signal 85 is input to the message signal input 80. A key signal 95, preferably from a random number generator, is input to the key signal input 90. The two signals 85 and 95 combine in the MIOC 30 to exit the encrypted message output 70 as an encrypted message signal 100. This is an "Exclusive Or" (XOR) encryption algorithm and a symmetric encryption algorithm. The message signal 85 and the key signal 95 are kept in phase by a software driver program.

To summarize, a coherent light signal is split between two paths 40 and 50. If neither a message signal 85 nor a key signal 95 is input, the divided light signal cancels itself out and no encrypted message signal 100 is emitted. When either a message signal 85 or a key signal 95 are input alone, the MIOC 30 emits an encrypted message signal 100 from the encrypted message output 70. When both a message signal 85 and a key signal 95 are input the light signals cancel each other out and no encrypted message signal 100 is emitted. In Figure 2, the message signal 85 is transformed by the key signal 95 to the encrypted message signal 100.

Thus, the simple encryption table in Figure 3 becomes apparent. In the 0,0 position of Figure 3, neither a message signal 85 nor a key signal 95 are input. Thus, no encrypted message signal 100 results. In the 0,1 position of the table, no message signal 85 is input and a key signal 95 is input. Thus, an encrypted message signal 100 results. Again, an "Exclusive Or" algorithm is depicted.

A method for encryption using interference from a coherent light source therefore becomes apparent. The method comprises the following steps:

Issuing a coherent light signal from a coherent light source 20 through a fiber optic link 25 to a multi-functional integrated optics chip 30;

Dividing the coherent light signal into two paths 40 and 50 within the multi-functional integrated optics chip 30;

Issuing pre-determined signals 85 and 95, respectively, from a message signal input 80 attached to one path 40 of the multi-functional integrated optics chip 30 and a key signal input 90 attached to the other path 50;

Recombining the divided light signal to create an encrypted message signal 100; and,

Issuing the encrypted signal from an encrypted message output 70.

Another user with an identical key signal 95 can decrypt the encrypted message signal 100 by using the above method and substituting the encrypted message signal 100 for the message signal 85. The resulting signal issued by the device will be the original message signal 85. By applying the key signal 95 to the encrypted message signal 100, the message signal 85 appears and can be read by a photo diode as any other digital signal or message clear text detailed in the prior art.

Therefore, the present invention has several advantages over the prior art. The preferred embodiments of the invention and the method of using them rapidly encrypt a message signal 85 as it is generated by simultaneously applying a key signal 95 using hardware instead of software. Translation from message signals to encrypted signals occurs rapidly in comparison to software data encryption

methods. The preferred embodiment of the invention can operate at 10 gigahertz (10GHz.) A user may still utilize prior art software encryption methods in addition to the present invention for increased security. The "Exclusive Or" algorithm detailed herein also doesn't require the use of public keys and/or prime numbers. In fact, when the key signal 95 comes from a random number generator, this invention creates a stream cipher that approximates a "one-time pad." A "one-time pad" is generally assumed to be an unbreakable method of encryption when a potential eavesdropper has no access to the one-time pad.

In each of the above embodiments, the different positions and structures of the present invention are described separately in each of the embodiments. However, it is the full intention of the inventor of the present invention that the separate aspects of each embodiment described herein may be combined with the other embodiments described herein. Those skilled in the art will appreciate that adaptations and modifications of the just-described preferred embodiment can be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention ~~may be practiced other than as specifically described herein.~~